We claim:

Sub A1 1. A computer program product for providing end-to-end user authentication for legacy host application access, said computer program product embodied on a computer-readable medium readable by a computing device in a computing environment and comprising:

computer-readable program code means for establishing a secure session from a client machine to a server machine using a digital certificate representing said client machine or a user thereof;

computer-readable program code means for storing said digital certificate at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol;

computer-readable program code means for passing said stored digital certificate from said server machine to a host access security system;

computer-readable program code means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

computer-readable program code means for accessing a stored password or a generated password substitute representing said located credentials; and

computer-readable program code means for using said stored password or said generated password substitute to transparently log said user on to a secure legacy host application executing at said host system.

2. The computer program product as claimed in Claim 1, wherein said digital certificate is an

X.509 certificate.

3. The computer program product as claimed in Claim 1 or Claim 2, wherein said communication protocol is a 3270 emulation protocol.

4. The computer program product as claimed in Claim 1 or Claim 2, wherein said communication protocol is a 5250 emulation protocol.

5. The computer program product as claimed in Claim 1 or Claim 2, wherein said communication protocol is a Virtual Terminal protocol.

6. The computer program product as claimed in Claim 3, wherein said host access security system is a Resource Access Control Facility (RACF) system.

7. The computer program product as claimed in Claim 1, wherein said server machine is a Web application server machine.

8. The computer program product as claimed in Claim 1, further comprising:

computer-readable program code means for requesting by said legacy host application, responsive to said computer-readable program code means for establishing said session, log on information for said user;

computer-readable program code means for responding to said request for log on

~~information by sending a log on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and~~

~~computer-readable program code means for substituting a user identifier associated with said located access credentials and said stored password or said generated passticket for said placeholders in said log on message.~~

~~9. The computer program product as claimed in Claim 7, further comprising:~~

~~computer-readable program code means for requesting by said legacy host application, responsive to said computer-readable program code means for establishing said session, log on information for said user; and~~

~~computer-readable program code means for responding to said request for log on information by supplying a user identifier associated with said located access credentials and said stored password or said generated passticket at said server machine.~~

Sub A1

~~10. A system for providing end-to-end user authentication for legacy host application access in a computing environment, comprising:~~

~~means for establishing a secure session from a client machine to a server machine using a digital certificate representing said client machine or a user thereof;~~

~~means for storing said digital certificate at said server machine;~~

~~means for establishing a session from said server machine to a host system using a legacy host communication protocol;~~

~~means for passing said stored digital certificate from said server machine to a host access~~

security system;

means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

means for accessing a stored password or a generated password substitute representing said located credentials; and

means for using said stored password or said generated password substitute to transparently log said user on to a secure legacy host application executing at said host system.

11. The system as claimed in Claim 10, wherein said digital certificate is an X.509 certificate.

12. The system as claimed in Claim 10 or Claim 11, wherein said communication protocol is a 3270 emulation protocol.

13. The system as claimed in Claim 10 or Claim 11, wherein said communication protocol is a 5250 emulation protocol.

14. The system as claimed in Claim 10 or Claim 11, wherein said communication protocol is a Virtual Terminal protocol.

15. The system as claimed in Claim 12, wherein said host access security system is a Resource Access Control Facility (RACF) system.

16. The system as claimed in Claim 10, wherein said server machine is a Web application server machine.

17. The system as claimed in Claim 10, further comprising:

means for requesting by said legacy host application, responsive to said means for establishing said session, log on information for said user;

means for responding to said request for log on information by sending a log on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

means for substituting a user identifier associated with said located access credentials and said stored password or said generated passticket for said placeholders in said log on message.

18. The system as claimed in Claim 16, further comprising:

means for requesting by said legacy host application, responsive to said means for establishing said session, log on information for said user; and

means for responding to said request for log on information by supplying a user identifier associated with said located access credentials and said stored password or said generated passticket at said server machine.

Sub A7

19. A method for providing end-to-end user authentication for legacy host application access in a computing environment, comprising the steps of:

establishing a secure session from a client machine to a server machine using a digital certificate representing said client machine or a user thereof;

storing said digital certificate at said server machine;

establishing a session from said server machine to a host system using a legacy host communication protocol;

passing said stored digital certificate from said server machine to a host access security system;

using, by said host access security system, said passed digital certificate to locate access credentials for said user;

accessing a stored password or a generated password substitute representing said located credentials; and

using said stored password or said generated password substitute to transparently log said user on to a secure legacy host application executing at said host system.

20. The method as claimed in Claim 19, wherein said digital certificate is an X.509 certificate.

21. The method as claimed in Claim 19 or Claim 20, wherein said communication protocol is a 3270 emulation protocol.

22. The method as claimed in Claim 19 or Claim 20, wherein said communication protocol is a 5250 emulation protocol.

23. The method as claimed in Claim 19 or Claim 20, wherein said communication protocol is a

Virtual Terminal protocol.

24. The method as claimed in Claim 21, wherein said host access security system is a Resource Access Control Facility (RACF) system.

25. The method as claimed in Claim 19, wherein said server machine is a Web application server machine.

26. The method as claimed in Claim 19, further comprising the steps of:

requesting by said legacy host application, responsive to said step of establishing said session, log on information for said user;

responding to said request for log on information by sending a log on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and

substituting a user identifier associated with said located access credentials and said stored password or said generated passticket for said placeholders in said log on message.

27. The method as claimed in Claim 25, further comprising the steps of:

requesting by said legacy host application, responsive to said step of establishing said session, log on information for said user; and

responding to said request for log on information by supplying a user identifier associated with said located access credentials and said stored password or said generated passticket at said server machine.

Add A